DOI: 10.18372/2307-9061.58.15326
УДК 343.9.024:004.056(045)

О. А. Клименко,
кандидат юридичних наук

М. В. Гуцалюк,
кандидат юридичних наук, старший науковий співробітник, доцент
ORCID ID: https://orcid.org/0000-0003-4496-5173

КРИМІНАЛЬНИЙ ОПОРТУНІЗМ КІБЕРЗЛОЧИННОСТІ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
Міжвідомчий науково-дослідний центр з проблем боротьби
з організованою злочинністю при РНБО України
Солом'янська площа, 1, 03035, Київ, Україна
E-mail: ms-kl18@ukr.net

Мета: *проаналізувати питання протидії кіберзлочинності під час пандемії COVID-19 та запропонувати шляхи посилення кібербезпеки в Україні.* ***Методи дослідження:*** *у процесі дослідження використані загальнофілософський, компаративістський та феноменологічний методи.* ***Обговорення:*** *обґрунтована необхідність в умовах зростання кількості й складності кіберзлочинів посилення міжнародної співпраці та вдосконалення чинного законодавства, зокрема, щодо електронних доказів, запропоновані методи захисту від кібершахраїв.* ***Результати:*** *виділені окремі види кіберзлочинів, на які слід звернути увагу під час пандемії коронавірусу; особлива увага приділена соціальній інженерії, кібершахрайству, APT-атакам на об'єкти критичної інфраструктури; надані пропозиції щодо вдосконалення чинного законодавства та пропозиції щодо протидії шахрайству.*

Ключові слова: *пандемія COVID-19; кіберзлочинність; шахрайство; кібербезпека; кібератака.*

Постановка проблеми та її актуальність. Одним із механізмів, що суттєво позитивно впливає на розвиток сучасного суспільства, є Інтернет, який є джерелом знань, засобом комунікації, інструментом цифрової економіки та управління.

Європейський Союз визначив поширення використання цифрових технологій одним із найважливіших пріоритетів свого розвитку та запровадив Цифрову ініціативу EU4Digital [1], що має на меті поширити Єдиний цифровий ринок Європейського Союзу на східні країни-партнери. Розвиток потенціалу цифрової економіки і суспільства приведе до економічного зростання, збільшення зайнятості населення, його доходів та надходжень до бюджету, створення нових робочих місць, поліпшення життя людей і розвитку бізнесу.

Ці кроки можуть додати 415 млрд євро щорічно на економічне зростання, конкуренцію, інвестиції та інновації в ЄС; створити кращий доступ для споживачів і підприємств, представників малого та середнього бізнесу на ринку до цифрових товарів і послуг по всій Європі; дати можливість розробити належні умови для поширення інноваційних послуг.

Цифрові технології стали ключовою складовою колективних зусиль по боротьбі з пандемією коронавірусу та у підтримці нових способів життя і праці, соціальної взаємодії в цей надзвичайний важкий час. Так, наприклад, штучний інтелект (ШІ) та суперкомп'ютери використовуються для виявлення закономірностей розповсюдження вірусу, розробки потенційних методів лікування та стратегій відновлення.

У Стратегії національної безпеки України, затвердженої Указом Президента України від

14 вересня 2020 року № 392/2020, зазначено, що поширення коронавірусної хвороби (COVID-19) виявило критичні проблеми в інформаційній сфері, в системах охорони здоров'я та соціального захисту, спричинило зростання безробіття. Пандемія руйнує усталений спосіб життя, загрожує продовольчому забезпеченню, перешкоджає вільному руху капіталу, товарів та робочої сили, завдає шкоди сфері послуг та, зрештою, підвищує протестні настрої у суспільствах і конфліктність у міжнародних відносинах.

Аналіз останніх досліджень і публікацій. Різні аспекти проблем боротьби з кіберзлочинністю були предметом дослідження таких вітчизняних науковців, як Ахтирська Н.М., Бутузов В.М., Гавловський В.Д., Голубєв В.О., Тітуніна К.В., Демедюк С.В., Савченко А.В., Хахановський В.Г., Шапочка С.В., Шеломенцев В.П. та ін. Проте багато питань, зокрема, особливості правопорушень під час пандемії, потребують подальшого дослідження та вирішення у практичній площині.

Виклад основного матеріалу. Значною загрозою для розвитку інформаційного суспільства є кіберзлочинність [2]. Втрати світової економіки через кіберзлочини і витрати на забезпечення захисту від них у цьому році перевищили 1 трлн доларів, тоді як ще два роки тому ця сума становила близько 600 млрд доларів. Про це йдеться у звіті виробника антивірусного програмного забезпечення McAfee [3]. Кіберзлочинці активно використовують тему COVID-19 для створення різноманітних злочинних схем. У той час, коли переважна частина людства намагалася виправити ситуацію, криміналітет в усьому світі почав використовувати цю проблему в своїх цілях.

Таку поведінку злочинців слід називати опортуністичною, адже під терміном опортунізм (франц. opportunism – пристосовництво, від лат. opportunus – зручний, вигідний, слушний) запропоновано розуміти поведінку, метою якої є отримання вигоди нечесним шляхом [4].

У статті видання Stabroek News «Coronavirus and opportunistic crime» [5] зазначається, що опортуністичні злочини – це злочини, які вчиняються внаслідок появи певних обставин, що створюють можливості для їхнього вчинення. Такі злочини, ймовірно, не були б вчинені, якби спочатку не виникли сприятливі обставини/умови.

Скажімо, раніше необхідність фізичного переміщення великої кількості готівки в конкретне місце, наприклад, доставка заробітної плати на заводи, створювала можливість для грабежів. Наразі, умови для вчинення таких злочинів значно зменшилися через створення більш безпечних методів транзакцій.

Злочинці, які використовують інформаційні технології, надзвичайно швидко адаптуються до змін у суспільстві для підвищення рівня кримінального прибутку. Вони почали більш ефективно використовувати традиційні методи кіберзлочинності, такі як соціальна інженерія, фішинг (спеціальна методика маніпуляції, яка допомагає змусити людину віддати зловмисникам необхідні дані) та шахрайство.

Так, компанія ESET, що є однією із провідних фірм у галузі інформаційної безпеки, повідомляє про виявлення нової APT-групи, яка викрадає конфіденційні документи державних установ у країнах Східної Європи та Балканського півострова. У 2020 році ця група кіберзлочинців у своїх фішингових кампаніях використовувала тему COVID-19, надсилаючи фішингові електронні листи різного типу (англ. APT – advanced persistent threat (постійна загроза підвищеної складності) – різновид складних кібератак з метою отримання несанкціонованого доступу до інформаційних систем та встановлення прихованого доступу до них для використання або контролю в майбутньому) [6].

Фахівці державного центру кібернетичної безпеки (NCSC), який є частиною британського розвідувального відомства, повідомляють, що зафіксовано цілу низку кібернападів ззовні, які мають на меті здирництво та використовують побоювання населення щодо розповсюдження коронавірусу. Йдеться про фейкові листи електронної пошти нібито від британських органів охорони здоров'я, які містять лінки на важливі поновлення комп'ютерної системи, а насправді при натисканні на них система отримувача заражається шкідливими комп'ютерними вірусами і наповнюється шпигунськими програмами.

Також злочинці удавали із себе представників Всесвітньої організації охорони здоров'я або британської державної служби охорони здоров'я NHS. При цьому жертвам шахрайства розсилалась фейкова інформація щодо устаткування та ліків, які нібито мали б допомогти у боротьбі з коронавірусом. При цьому кіберзлочинці вимагали фінансової допомоги для ведення досліджень з вироблення вакцини проти цього вірусу.

Британська розвідка повідомляє, що хакерською групою, яка використовує глобальну кризу, зв'язану з коронавірусом, є кіберугрупування Hades.

У ФРН кіберзлочинці намагаються обманним шляхом отримати державну допомогу для підприємств, що постраждали від карантинних заходів.

Співробітники німецької поліції та спецслужб виявили десятки шахрайських сайтів німецькою мовою, метою яких було привласнення державної фінансової допомоги для підприємств, що постраждали від наслідків обмежувальних заходів.

Зокрема, на домені wirtschaft-nrw.info кіберзлочинці повністю відтворили офіційний сайт Міністерства економіки федеральної землі Північний Рейн-Вестфалія. Фейк містив усі розділи і вбудовані елементи справжнього сайту, включно з розділом про боротьбу з фейками та економічними злочинами [7].

Європейські правоохоронні органи провели розслідування десяти випадків шахрайства з технічною підтримкою. Спочатку зловмисники спілкувались зі своїми жертвами телефоном, видаючи себе за технічних працівників центру підтримки програмного забезпечення. Під приводом того, що їхній комп'ютер та/або мобільний пристрій «заражені» шкідливим програмним забезпеченням, злочинці попросили потерпілих встановити програмне забезпечення для віддаленого доступу, щоб нібито вирішити проблему.

Таким чином, злочинці отримали повний доступ до комп'ютера або мобільного пристрою, а отже, до збережених на пристроях персональних даних. Використовуючи персональні дані, зловмисники перераховували гроші з електронних банківських рахунків (електронного банкінгу) на банківські рахунки, що контролюються ними самими або їхніми співучасниками. У багатьох випадках вони навіть вимагали встановлення програм віддаленого управління на мобільних телефонах потерпілих, щоб можна було отримувати текстові повідомлення (SMS) з одноразовими кодами (OTP), які фінансові установи надсилають з міркувань безпеки [8].

Широке використання технологій та зростаючі темпи підключення до Інтернету в усьому світі в поєднанні з постійним розвитком нових технологій, які забезпечують анонімність в Інтернеті, дають змогу кіберзлочинності бути низькоризиковою та високоприбутковою справою. Через це у два найближчі десятиліття кіберзлочинність залишатиметься однією з серйозних проблем для розвитку суспільства як в Україні, так і в більшості країн світу [9].

Пандемія COVID-19 посилила зростання специфічних видів кіберзлочинів, оскільки громадяни та бізнес активно шукають необхідну інформацію про заходи профілактики й лікування від небезпечного вірусу. Відповідно, зросла кількість нових доменів та вебсайтів, зв'язаних із COVID-19. Одночасно з початком спалаху пандемії кіберзлочинці активно експлуатують цю проблему, створюючи фейкові сайти та спонукаючи людей купувати фальсифіковані ліки, добавки і вакцини. За даними, зібраними та проаналізованими Atlas VPN, кількість фішингових вебсайтів під час карантину COVID-19 зросла на 350% [10].

Пандемія також породила широкі кампанії щодо дезінформації стосовно способів поширення вірусу, методів лікування та профілактики. Розповсюдження фейкових новин стало однією з вирішальних загроз під час пандемії, вони надають нові можливості для кіберзлочинців у впровадженні своїх схем, а також підривають довіру до державних установ та заходів. Так, Служба безпеки України викрила і припинила діяльність понад 450 інтернет-агітаторів, які поширювали неправдиву інформацію про коронавірус в Україні. Пік поширення фейків і панічних настроїв спостерігався на початку карантинних заходів [11].

Особливого кіберзахисту потребують офіційні інституції, задіяні в подоланні проблеми поширення вірусу, які зазнають потужних кібератак. Так, наприклад, у листопаді 2020 року хакери із КНДР намагалися проникнути в системи британського виробника ліків і розробника вакцини від COVID-19 AstraZeneca. Як повідомило агентство Reuters із посиланням на власні джерела, хакери видавали себе за рекрутерів і за допомогою LinkedIn та WhatsApp зверталися до персоналу AstraZeneca з неправдивими пропозиціями про роботу. Після цього вони надіслали документи з нібито посадовими інструкціями, які містили шкідливий код, призначений для доступу до комп'ютера потерпілої особи.

Атаки були спрямовані на широке коло осіб, що включало співробітників, які працюють над дослідженнями COVID-19. Проте, за даними співробітників видання, ці спроби не вдалися [12].

А вже у грудні 2020 року унаслідок хакерської атаки на Європейську агенцію лікарських засобів (EMA), розташовану в Амстердамі, були викрадені документи, зв'язані з допуском на ринок вакцини від коронавірусу німецької компанії BioNTech та американської Pfizer. Експерти вважають, що за цим стоять спецслужби окремих держав [13].

У зв'язку із різким зростанням Інтернет-активності значно збільшилася кількість шахрайських дій і в Україні. Так, 80% від усіх звернень громадян у кіберполіцію становлять повідомлення про шахрайські дії в Інтернеті [14].

За словами фахівців, найбільш поширеними видами шахрайства у віртуальному просторі є продаж неіснуючих товарів, а також фішингові онлайн-магазини.

Найчастіше злодії ошукують громадян, продаючи неіснуючі товари на майданчиках оголошень або в соцмережах. Як правило, в таких випадках головною умовою покупки є повна передоплата за товар.

Ще однією поширеною схемою шахраїв є створення фішингових ресурсів, які зовні схожі на популярні Інтернет-магазини. Оплачуючи товари на таких сайтах покупець не тільки залишається без бажаного товару, а й передає дані банківської картки аферистові.

Слід зазначити, що багато шахраїв «працюють» безпосередньо з місць позбавлення волі та мають значний кримінальний досвід, а тому звернення потерпілих безпосередньо до шахраїв з проханням повернути кошти не мають жодного ефекту.

Як повідомляє прес-служба «Укрпошти», 5 грудня 2020 року в мережі з'явилася інформація, що користувачі поштових операторів отримують листи про необхідність доплатити мито, в тому числі від імені «Укрпошти».

Компанія закликає не реагувати на них, адже це шахрайська розсилка, спрямована на заволодіння даними банківських карток. За вказаним у листі посиланням користувачі потрапляють на фальшивий сайт, який імітує офіційний інтернет-сайт «Укрпошти», для здійснення додаткової оплати. Насправді таким чином шахраї збирали дані банківських карток для подальшого незаконного зняття коштів [15].

У зв'язку з тим, що під час пандемії багато підприємств зазнають збитків, їхні власники намагаються знаходити нові цілі інвестиційної діяльності. Цим також вдало користуються кіберзлочинці. Так, за повідомленням Офісу Генерального прокурора України, в Києві правоохоронці припинили діяльність шахрайських call-центрів, які під виглядом інвестиційних посередників обманювали громадян ЄС. Злочинна схема працювала близько трьох років, у ній брало участь близько тисячі співробітників-операторів. Організатори шахрайської схеми використовували завчасно створені вебсайти з торгівлі валютою, криптовалютою, цінними паперами, золотом і нафтою. Під виглядом інвестиційних посередників вони залучали кошти громадян Північної і Центральної Європи, обіцяючи їм отримання надприбутків у короткостроковій перспективі.

У дослідженні Європолу IOCTA шахрайство з Інтернет-інвестиціями визначили одним із найбільш швидкозростаючих злочинів за останні 12 місяців, що призвело до мільйонних збитків. Постраждали тисячі осіб в усіх країнах ЄС. Багато держав-учасниць ЄС вперше стали свідками такого шахрайства.

Пропонуючи такі товари як криптовалюти, алмази або золото злочинці обіцяють жертвам надзвичайну фінансову віддачу від своїх інвестицій. При цьому кіберзлочинці залучають жертв за допомогою вебсайтів, які демонструють «високу» інвестиційну вигоду. На жаль, деякі потерпілі втратили всі свої заощадження, перш ніж зрозуміли, що стали жертвою шахрайства.

Низка випадків онлайн-шахрайства з інвестиціями продемонструвала значний рівень складності, оскільки за цими схемами стоять великі мережі компаній-оболонок, а також складне програмне забезпечення й комунікаційні тактики.

Злочинці, як правило, націлюються на жертв через соціальні мережі, використовуючи дезінформацію. На шахрайські вебсайти про інвестиції люди натрапляють також через пошукові системи. Інтернет-шахрайство з інвестиціями важко розслідувати, оскільки злочинці створюють складні міжнародні схеми компаній, які мають юридичну форму, що охоплюють кілька юрисдикцій. Групи, які стоять за цими схемами, не просто визначити, частково завдяки використанню інструментів анонімізації, підроблених телефонних номерів та законних вебсайтів.

Враховуючи стрімке зростання інвестиційного шахрайства в багатьох державах-учасницях ЄС, правоохоронні органи очікують, що цей вид шахрайства буде і далі розповсюджуватися [8].

Таким чином, кібершахрайство, викрадення персональних даних, кібершпигунство та інші правопорушення у кіберпросторі створюють серйозну загрозу національній безпеці України, особливо в складний час боротьби з пандемією коронавірусу. Підвищення активізації кіберзлочинів слід очікувати при проведенні щеплення проти вірусу. Тому інформаційну структуру медичних закладів варто віднести до об’єктів критичної інформаційної структури з відповідним рівнем кіберзахисту.

Для ефективної протидії як кібершахрайству, так і в цілому кіберзлочинності сьогодні залишається актуальною імплементація положень Конвенції про кіберзлочинність 2001 року, зокрема ст. 16 «Термінове збереження комп’ютерних даних, які зберігаються» та ст. 17 «Термінове збереження і часткове розкриття даних про рух інформації», а також вдосконалення методів використання електронних доказів, законопроєкти щодо яких були внесені на розгляд Верховної Ради України у вересні 2020 року. Також необхідно вдосконалити механізми міжнародного співробітництва, зокрема, щодо обміну оперативною інформацією та участі у міжнародних слідчих групах.

Висновки. Злочинці постійно пристосовуються до змін у суспільстві та вигадують нові методи і способи вчинення правопорушень. Водночас, проблема шахрайства, зокрема у кіберпросторі, внаслідок своєї динаміки становить загрозу розвитку інформаційного суспільства в Україні. У зв’язку з цим зазначена тенденція потребує свого висвітлення у новій Стратегії кібербезпеки України. Важливе значення має високопрофесійна підготовка відповідних фахівців підрозділів боротьби з кіберзлочинністю, а також підвищення їхньої кваліфікації з питань впровадження системи виявлення кіберзлочинів.

Для виявлення шахрайських дій експерти рекомендують:

1) використовувати тільки перевірені ресурси і переконатися в правильності назви необхідного сайту. Один непомітний символ у назві сайту на панелі адреси може означати, що ви потрапили на фішинговий сайт;

2) не передавати нікому дані своєї банківської картки (особливо CVV-код і пін-код), адже працівники банку ніколи не запитують таку інформацію;

3) рекомендується завжди використовувати накладний платіж, щоб виключити шанси шахраїв заволодіти вашими коштами.

Для перевірки незнайомих реквізитів можна скористатися сайтом кіберполіції, де в розділі «Стоп Фрауд» є можливість перевірити номер телефону, банківську карту і посилання на сумнівний сайт. Можливо, шахраї вже є в базі кіберполіції.

Також буде корисним надання просвітницької інформації з питань кібергігієни у навчальних закладах та проведення інформаційних кампаній, які, наприклад, проводив Національний банк з протидії платіжному шахрайству.

Література

1. Єдиний цифровий ринок ЄС. URL: https://eufordigital.eu/uk/discover-eu/eu-digital-single-market/

2. Klymenko Olga A., Gutsaliuk Mykhailo V., Savchenko Andrii V. (2020). Combater o cibercrime como pré-requisito para o desenvolvimento da sociedade digital. *JANUS.NET e-journal of International Relations*. Vol. 11. № 1. Maio-Outubro, 2020. Consultado [em linha] em data da última consulta, pp.18-29. URL: https://doi.org/10.26619/1647-7251.11.1.2

3. The Hidden Costs of Cybercrime. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

4. Словник іншомовних слів / за ред. члена-кореспондента АН УРСР О.С. Мельничука. Київ: Головна редакція «Українська радянська енциклопедія», 1977. 776 с.

5. Coronavirus and opportunistic crime. URL: https://www.stabroeknews.com/2020/04/14/opinion / editorial/coronavirus-and-opportunistic-crime/

6. Кіберзлочинці використовують тему COVID-19 в атаках на державні установи Європи. URL: https://eset.ua/ua/news/view/837/kiberprestupniki-ispolzuyut-temu-covid-19-v-atakakh-na-gosudarstvennyye-uchrezhdeniya-yevropy

7. Як шахраї в Німеччині використовують коронавірус у своїх цілях. URL: https://www.dw.com/uk

8. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol. europa.eu/iocta-report

9. Гуцалюк М.В. Шляхи посилення спроможностей правоохоронних та інших державних органів у сфері боротьби з кіберзлочинністю. *Інформація і право*. 2020. № 3(34). С. 75–87.

10. Google Registers a 350 % Increase in Phishing Websites Amid Quarantine. URL: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine

11. Поширювали фейки про Covid-19: СБУ викрила понад 450 інтернет-агітаторів. URL: https://fakty.com.ua/ua/ukraine/20201209-poshyryuvaly-fejky-pro-covid-19-sbu-vykryla-ponad-450-internet-agitatoriv/

12. Хакери з Північної Кореї здійснили атаку на розробника вакцин від COVID-19. ЗМІ. URL: https://zik.ua/news/world/khakery_z_pivnichnoi_korei_zdiisnyly_ataku_na_rozrobnyka_vaktsyn_vid_covid_19__zmi_988603

13. Викрадення документів щодо COVID-вакцини: що відомо про хакерську атаку. URL: https://www.dw.com/uk/vykradennia-dokumentiv-shchodo-covid-vaktsyny-shcho-vidomo-pro-khakersku-ataku/a-55892885?maca=ukr-rss-ukrnet-ukr-all-3816-xml

14. З початку 2020 року до кіберполіції надійшло понад 25 тисяч звернень щодо Інтернет-шахрайства. URL: https://cyberpolice.gov.ua/news/z-pochatku--roku-do-kiberpolicziyi-nadijshlo-ponad--tysyach-zvernen-shhodo-internet-shaxrajstva-6472/

15. «Укрпошта» обратилась в киберполицию из-за мошеннических сообщений об оплате пошлин. URL: https://biz.censor.net/n3235880

References

1. Iedynyi tsyfrovyi rynok YeS. URL: https://eufordigital.eu/uk/discover-eu/eu-digital-single-market/

2. Klymenko Olga A., Gutsaliuk Mykhailo V., Savchenko Andrii V. (2020). Combater o cibercrime como pré-requisito para o desenvolvimento da sociedade digital. *JANUS.NET e-journal of International Relations*. Vol. 11. № 1. Maio-Outubro, 2020. Consultado [em linha] em data da última consulta, pp. 18-29. URL: https://doi.org/10.26619/1647-7251.11.1.2

3. The Hidden Costs of Cybercrime. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

4. Slovnyk inshomovnykh sliv / za red. chlena-korespondenta AN URSR O.S. Melnychuka. Kyiv: Holovna redaktsiia «Ukrainska radianska entsyklopediia», 1977. 776 s.

5. Coronavirus and opportunistic crime. URL: https://www.stabroeknews.com/2020/04/14/opinion/editorial/coronavirus-and-opportunistic-crime/

6. Kiberzlochyntsi vykorystovuiut temu COVID-19 v atakakh na derzhavni ustanovy Yevropy. URL: https://eset.ua/ua/news/view/837/kiberprestupniki-ispolzuyut-temu-covid-19-v-

atakakh-na-gosudarstvennyye-uchrezhdeniya-yevropy

7. Iak shakhrai v Nimechchyni vykorystovuiut koronavirus u svoikh tsiliakh. URL: https://www.dw.com/uk

8. Internet Organised Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/iocta-report

9. Hutsaliuk M.V. Shliakhy posylennia spromozhnostei pravookhoronnykh ta inshykh derzhavnykh orhaniv u sferi borotby z kiberzlochynnistiu. *Informatsiia i pravo*. 2020. № 3(34). S. 75–87.

10. Google Registers a 350% Increase in Phishing Websites Amid Quarantine. URL: https://atlasvpn.com/blog/google-registers-a-350-increase-in-phishing-websites-amid-quarantine

11. Poshyriuvaly feiky pro Covid-19: SBU vykryla ponad 450 internet-ahitatoriv. URL: https://fakty.com.ua/ua/ukraine/20201209-poshyryuvaly-fejky-pro-covid-19-sbu-vykryla-ponad-450-internet-agitatoriv/

12. Khakery z Pivnichnoi Korei zdiisnyly ataku na rozrobnyka vaktsyn vid COVID-19. ZMI. URL: https://zik.ua/news/world/khakery_z_pivnichnoi_korei_zdiisnyly_ataku_na_rozrobnyka_vaktsyn_vid_covid_19__zmi_988603

13. Vykradennia dokumentiv shchodo COVID-vaktsyny: shcho vidomo pro khakersku ataku. URL: https://www.dw.com/uk/vykradennia-dokumentiv-shchodo-covid-vaktsyny-shcho-vidomo-pro-khakersku-ataku/a-55892885?maca=ukr-rss-ukrnet-ukr-all-3816-xml

14. Z pochatku 2020 roku do kiberpolitsii nadiishlo ponad 25 tysiach zvernen shchodo Internet-shakhraistva. URL: https://cyberpolice.gov.ua/news/z-pochatku-roku-do-kiberpolicziyi-nadijshlo-ponad-tysyach-zvernen-shhodo-internet-shaxrajstva-6472/

15. «Ukrposhta» obratylas v Kyberpolytsyiu yz-za moshennycheskykh soobshchenyi ob oplate poshlyn. URL: https://biz.censor.net/n3235880

O. Klymenko, M. Gutsalyuk

CRIMINAL OPPORTUNISM OF CYBER CRIME AS A THREAT TO NATIONAL SECURITY OF UKRAINE

National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
Interagency Research Center for Combating Organized Crime
at the National Security and Defense Council of Ukraine
Solomjanska Square, 1, 03035, Kyiv, Ukraine
E-mail: ms-kl18@ukr.net

Purpose: *to analyze the issues of combating cybercrime during the COVID-19 pandemic and to suggest ways to strengthen cybersecurity in Ukraine.* ***Methods****: general philosophical, comparative and phenomenological methods are used in the research process.* ***Results:*** *some types of cybercrimes that should be considered during a coronavirus pandemic have been identified; special attention is paid to social engineering, cyber-fraud, APT-attacks on critical infrastructure; proposals for improving the current legislation, and proposals for combating fraud.* ***Discussion****: the need to strengthen international cooperation and improve the current legislation, in particular on electronic evidence, in the conditions of increasing the number and complexity of cybercrimes is substantiated, methods of protection against cybercriminals are proposed.*

The researchers believe that given that the coronavirus pandemic will not disappear in the near future and the number of remote users will increase, the number of cybercrimes will increase accordingly.

The authors conclude that the problem of fraud, particularly in cyberspace, due to its dynamics poses a threat to the development of the information society in Ukraine. In this regard, this trend needs to be covered in the new Cyber Security Strategy of Ukraine. Professional training of relevant specialists of cybercrime units is highly important, as well as the implementation of a system to improve the detection of cybercrime. It will also be useful to provide educational information on cyber hygiene in schools and information campaigns, to combat payment fraud.

In addition, the authors recommend detecting and combating fraud:

1) use only proven resources and make sure the name of the required site is correct. One inconspicuous character in the site name in the address bar may indicate that you are on a phishing site;

2) do not pass on your bank card details (especially CVV-code and pin-code) to anyone, because bank employees never ask for such information;

3) it is recommended to always use cash on delivery to eliminate the chances of fraudsters seizing your funds.

Keywords: *COVID-19 pandemic; cybercrime; fraud; cyber security; cyber attack.*